

# UNITED STATES ENVIRONMENTAL PROTECTION AGENCY OFFICE OF THE INSPECTOR GENERAL OFFICE OF INVESTIGATIONS

1200 PENNSYLVANIA AVENUE NW ARLINGTON, VA 20460

#### REFERRED FOR ACTION REPORT OF INVESTIGATION CONCERNING

UNKNOWN SUBJECT: IP(b) (7)(E) (EXTERNAL FIREWALL (b) (7)(E) 2009-CS-0145

Т	CABLE OF CONTENTS
Narrative Entities and Individuals Prosecutive Status Exhibits	Section A Section B Section C
Distribution:	Approvals:
DAIGI STEPHEN NESBITT, AIGI	Special Agent
	Special Agent in Charge

## OFFICE OF INSPECTOR GENERAL OFFICE OF INVESTIGATIONS

**CASE NO.:** 2009-CS-0145 **DATE OPENED:** 09/24/2009

CASE TITLE: UNKNOWN SUBJECT:

**CASE AGENT:** 

 $IP^{(b)}(7)(E)$ 

(EXTERNAL FIREWALL

(b) (7)(E)

CASE CATEGORY: COMPUTER INTRUSION OFFICE:

OFFICE OF

INVESTIGATIONS -

NERC

PHILADELPHIAEASTER N RESOURCE CENTER

JOINT AGENCIES: None

JURISDICTION: MARYLAND

#### SECTION A - NARRATIVE

#### **Predication**

On August 13, 2009 the Environmental Protection Agency (EPA), Office of the Inspector General (OIG), Office of Investigations (OI) received notification from Computer Sciences Corporation (CSC) of an intrusion detected on the EPA's (b) (7)(E) application development site.

Investigation revealed that an alert was detected by the CSC (b) (7)(E) on August 12, 2009 at 4:00PM. An intrusion was detected from several IP addresses with up to 10,000 outbound events noted from one single system. In depth review of the CSC (b) system reports revealed unidentified attackers had made 10776 attempts to exploit a (b) (7)(E)

The CSC (b) detected inbound connection attempts from multiple Internet Protocol (IP) addresses (b) (7)(E)(7)

#### Possible violations:

- 1. TITLE 18 USC SEC 1030, Fraud and related activity in connection with computers
- 2. TITLE 18 USC SEC 1029, Fraud and related activity in connection with access devices

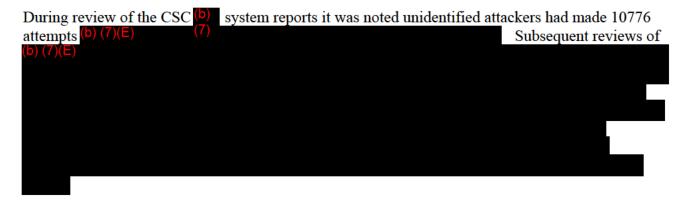
#### Impact/Dollar Loss

2

No dollar loss; Potential threat & vulnerability to EPA Information Exchange Network; Flawed & vulnerable testing procedures, No due diligence

#### **Synopsis**

Investigation and forensic analysis revealed an intrusion was detected which targeted several Agency systems utilized by CSC to perform testing of applications. These systems were created, maintained and operated as a developmental network by CSC within their corporate network. Verification was obtained that no CBI or other sensitive data was available to the intruders on the systems compromised. The entire severity and impact was not determined based on the limited availability and destruction of digital evidence for analysis.



#### **Details**

Allegation 1: TITLE 18 USC SEC 1030, Fraud and related activity in connection with computers

```
Allegation 1 Findings: Forensic analysis and review of CSC(b) revealed numerous inbound connection attempts (b) (7)(E)

(b) (5), (b) (7)(E)

revealed numerous inbound review of CSC(b) revealed numerous inbound review of CSC(c) revealed numerous inbound reve
```

Allegation 2: TITLE 18 USC SEC 1029, Fraud and related activity in connection with access devices

```
Allegation 2 Findings: Forensic analysis and review of (b) (7)(E)

(b) (5), (b) (7)(E)

Investigation failed to identify individuals who compromised system access devices for the test network and systems.
```

#### **Disposition**

During the course of investigation it was discovered that the intrusion occurred against the CSC company domain where they were testing a upgrade. During the early phase of the investigation the contract was transferred to CGI federal for continued execution. In that transition data and systems transferred to CGI federal were unrecoverable.

(b) (7)(E)

No other hostile activity has been reported. This investigation is being closed.

#### SECTION B - ENTITIES AND INDIVIDUALS

Name of Person: UNKNOWN

Title & Company: UNKNOWN & UNKNOWN

Role: Subject

**Business Address:** UNKNOWN, **Business Phone:** UNKNOWN

**EPA Employee:** N

-----

#### SECTION C - PROSECUTIVE STATUS

ADMIN/CRIMINAL/CIVIL ACTION(S): UNKNOWN

Investigation failed to identify individuals who penetrated the CSC (b) (7)(E) network and systems.

No referral is made for action.

#### **EXHIBITS**

DESCRIPTION	EXHIBIT
EPA Form 2720-15 - Date Attached: 10/13/2009 Time Attached: 4:03:30	1
EPA Form 2720-15 - Date Attached: 10/13/2009 Time Attached: 4:05:50  EPA Form 2720-15 - Date Attached: 10/13/2009 Time Attached: 4:11:15	2
EPA Form 2720-15 - Date Attached: 10/13/2009 Time Attached: 4:13:39	3
EPA Form 2720-15 - Date Attached: 10/13/2009 Time Attached: 4:36:56	4
EPA Form 2720-15 - Date Attached: 10/13/2009 Time Attached: 4:15:21	5
EPA Form 2720-15 - Date Attached: 9/18/2009 Time Attached: 2:38:34	6
EPA Form 2720-15 - Date Attached: 9/18/2009 Time Attached: 2:40:15	7
EPA Form 2720-15 - Date Attached: 9/18/2009 Time Attached: 3:03:10	8
(b) (7) report	9
EPA Form 2720-15 - Date Attached: 10/7/2009 Time Attached: 3:47:19	10
EPA Form 2720-15 - Date Attached: 10/7/2009 Time Attached: 3:58:40	11
EPA Form 2720-15 - Date Attached: 10/7/2009 Time Attached: 4:00:46	12
Tiger Documents 1	13



#### UNITED STATES ENVIRONMENTAL PROTECTION AGENCY OFFICE OF THE INSPECTOR GENERAL OFFICE OF INVESTIGATIONS

TWO POTOMAC YARD 2733 SOUTH CRYSTAL DRIVE ARLINGTON, VA 22202

#### FINAL REPORT OF INVESTIGATION CONCERNING

UNKNOWN SUBJECT: UNAUTHORIZED ACCESS TO MULTIPLE EPA SERVERS (LAS VEGAS) OCI-AR-2011-CAC-2772

#### TABLE OF CONTENTS

Narrative Entities and Individuals Prosecutive Status Exhibits	Section A Section B Section C
Distribution: File	Approvals:  Senior Special Agent Electronic Crimes Division
	Special Agent in Charge Electronic Crimes Division

## OFFICE OF INSPECTOR GENERAL OFFICE OF INVESTIGATIONS

CASE NO.: OCI-AR-2011-CAC-2772 DATE OPENED: 3/25/2011

CASE TITLE: UNKNOWN SUBJECT: CA

**CASE AGENT:** 

UNAUTHORIZED

ACCESS TO MULTIPLE EPA SERVERS (LAS

VEGAS)

CASE CATEGORY: COMPUTER INTRUSION OFFICE: OFFICE OF

INVESTIGATIONS ELECTRONIC CRIMES

DIVISION

JOINT AGENCIES: None

JURISDICTION: NEVADA

#### **SECTION A - NARRATIVE**

#### **Predication**

This investigation was opened on March, 25, 2011, The Office of Cyber Investigations and Homeland Security (OCI) received notification that suspicious network logins to EPA financial payment systems were occurring on several servers in Las Vegas, Nevada. The systems included in the reported suspicious activity were (b) (7)(E)

#### Possible violations:

1. TITLE 18 USC SEC 1030, Fraud and related activity in connection with computers

#### Impact/Dollar Loss

This incident had the potential to impact all EPA financial systems and the physical security of environmental incident response and research facilities.

#### **Synopsis**

The investigation failed to determine the source of the unauthorized user account activity identified in the Las Vegas Finance center computer systems. Anomalies found in the system logs by EPA IT administrators compared with other available data failed to uncover the source or cause of the activity.

Forensic analysis of data available discovered an unidentified encrypted file that was unable to be opened for further analysis.

#### **Details**

<u>Allegations</u>: Violation of TITLE 18 United States Code Section 1030(a)-(4), Fraud and related activity in connection with computers, exceeding authorized access by a detailed Public Health Service employee

<u>Allegations Findings</u>: Investigation was unable to substantiate the allegation. No conclusive evidence of criminal activity could be determined.

#### **Disposition**

Due to the lack of conclusive evidence of criminal activity, no referral for prosecution or any course of legal action was made.

#### SECTION B - ENTITIES AND INDIVIDUALS

Name of Person: Unknown

Title & Company: Role: Subject Business Address: Business Phone: EPA Employee: N

-----

#### **SECTION C – PROSECUTIVE STATUS**

ADMIN/CRIMINAL/CIVIL ACTION(S): NONE

#### **EXHIBITS**

DESCRIPTION	EXHIBIT
Memorandum of Activity for Imaging, Dated February 3, 2011	1
Memorandum of Interview for , Dated February 4, 2011	2
Memorandum of Activity for Network Monitoring, Dated February 5, 2011	3
Memorandum of Activity for Imaging, Dated February 5, 2011	4
Memorandum of Interview for Dated September 21, 2011	5



## UNITED STATES ENVIRONMENTAL PROTECTION AGENCY OFFICE OF INSPECTOR GENERAL

TWO POTOMAC YARD 2733 SOUTH CRYSTAL DRIVE ARLINGTON, VA 22202

CASE #: OCI-AR-2011-CAC-2783 CROSS REFERENCE #:

**TITLE: Unknown Intrusion into EPA** 

System (b) (7)(E)

**CASE AGENT** (if different from prepared by):

#### SHORT-FORM REPORT OF INVESTIGATION

**PERIOD COVERED:** FROM 4/15/2011 TO 1/10/2013

STATUS OF CASE: CLOSED INVESTIGATION

**JOINT AGENCIES:** None

**DISTRIBUTION:** SAC

AIGI MICHAEL DAGGETT

File

**PREDICATION:** On April 11, 2011, the Office of Cyber Investigations and Homeland Security (OCI) discovered that an EPA system had been compromised by unknown individuals.

**DETAILS:** Due to the sensitive nature of the investigation, the details are not being reported in our electronic case management system. See the hard copy case file for the closing report of investigation.

<u>Allegation 1</u>: Title 18 USC SEC 1029 Fraud and related activity in connection with access devices.

Allegation 1 Findings: See hard copy case file

Allegation 2: Title 18 USC SEC 1030 Fraud and related activity in connection with computers.

Allegation 1 Findings: See hard copy case file

**DISPOSITION:** See hard copy case file

**EXHIBITS:** None



#### UNITED STATES ENVIRONMENTAL PROTECTION AGENCY OFFICE OF THE INSPECTOR GENERAL OFFICE OF INVESTIGATIONS

TWO POTOMAC YARD 2733 SOUTH CRYSTAL DRIVE ARLINGTON, VA 22202

#### FINAL REPORT OF INVESTIGATION CONCERNING

### UNKNOWN SUBJECT(S) – UNAUTHORIZED EPA LAN ACCESS OCI-AR-2012-CAC-0014

#### TABLE OF CONTENTS

111222 01	COTTENTS
Narrative Entities and Individuals Prosecutive Status Exhibits	Section A Section B Section C
Distribution: File	Approvals:  Special Agent
	Special Agent in Charge

## OFFICE OF INSPECTOR GENERAL OFFICE OF INVESTIGATIONS

CASE NO.: OCI-AR-2012-CAC-0014 DATE OPENED: 11/01/2011

CASE TITLE: UNKNOWN SUBJECT(S) CASE AGENT:

- UNAUTHORIZED EPA

LAN ACCESS

CASE CATEGORY: COMPUTER INTRUSION OFFICE: OFFICE OF

INVESTIGATIONS

JOINT AGENCIES: None

JURISDICTION: DISTRICT OF COLUMBIA

#### SECTION A - NARRATIVE

#### Predication

This investigation was opened on November 1, 2011, based on the notification by

Security Management Division, EPA, Washington, DC, of a security violation concerning EPA's Local Area Network committed by unknown person(s).

According to SMD was notified that unknown individual(s) were accessing EPA's LAN allegedly with a personal computer. The access was occurring in the EPA East and Ariel Rios North Buildings, Washington, DC.

The access was occurring in the EPA East and Ariel Rios North Buildings, Washington, DC.

The access was occurring in the EPA LAN had been accessed so far.

#### Possible violations:

1. TITLE 18 USC SEC 1029, Fraud and related activity in connection with access devices

#### Impact/Dollar Loss

The impact of this incident represents a compromise of the command and control of EPA systems and the EPA network.

#### **Synopsis**

On November 1, 2011, Security

Management Division, EPA, Washington, DC reported a security violation concerning EPA's Local

Area Network (LAN) committed by unknown person(s). According to that unknown individual(s) were accessing EPA's LAN allegedly with a personal computer. The

access was occurring in the EPA East and Ariel Rios North Buildings, Washington, DC. related there have been at least six times the EPA LAN had been accessed so far.



Although the allegations were substantiated as unauthorized access was documented in EPA's LAN records, the investigation was unable to positively identify the individual(s) who gained access to the EPA data networks through physical means to steal/maintain access to EPA internet resources.

#### Details

Allegation 1: 18 USC 1029 Fraud and related activity in connection with access devices.

Findings: Unknown individual(s), without proper authorization, gained access to the EPA physical LAN closets networks and utilized network resources.

#### **Disposition**

Investigation failed to identify the individual(s) who gained access to the EPA's network. No referral for prosecution was made.

#### SECTION B – ENTITIES AND INDIVIDUALS

Name of Person: Unknown

Title & Company: Role: Subject **Business Address: Business Phone:** EPA Employee: N

#### SECTION C – PROSECUTIVE STATUS

ADMIN/CRIMINAL/CIVIL ACTION(S): None

#### **EXHIBITS**

DESCRIPTION	EXHIBIT
MOI Interview of , August 24, 2011	1
MOI Interview of September 6, 2011	2
MOI Interview of , October 28, 2011	3
MOA Review of Security Logs, February 9, 2012	4
MOA Attempt to contact May, 30 2013	5

# U.

## UNITED STATES ENVIRONMENTAL PROTECTION AGENCY OFFICE OF INSPECTOR GENERAL

TWO POTOMAC YARD 2733 SOUTH CRYSTAL DRIVE ARLINGTON, VA 22202

CASE #: OCI-AR-2012-CAC-0035 CROSS REFERENCE #:

TITLE: COMPROMISE OF EPA

SYSTEMS (FO)

**CASE AGENT** (if different from prepared by):

#### SHORT-FORM REPORT OF INVESTIGATION

**PERIOD COVERED:** FROM 1/18/2012 TO 4/12/2013

STATUS OF CASE: CLOSED INVESTIGATION

**JOINT AGENCIES: FBI** 

**DISTRIBUTION:** SAC

AIGI MICHAEL DAGGETT

File

**PREDICATION:** On December 26, 2011, The Office of Cyber Investigations and Homeland Security (OCI) received notification from Computer Security Incident Response Center (CSIRC), that EPA users had been compromised by navigating to foreign websites.

**DETAILS:** Due to the sensitive nature of the investigation, the details are not being reported in our electronic case management system. See the hard copy case file for the closing report of investigation.

<u>Allegation 1</u>: Title 18 USC SEC 1029 Fraud and related activity in connection with access devices.

Allegation 1 Findings: See hard copy case file

Allegation 2: Title 18 USC SEC 1030 Fraud and related activity in connection with computers.

Allegation 1 Findings: See hard copy case file

**DISPOSITION:** Investigation was not able to determine the identity of the intruders. A referral for prosecution was not made.



## UNITED STATES ENVIRONMENTAL PROTECTION AGENCY OFFICE OF INSPECTOR GENERAL

TWO POTOMAC YARD 2733 SOUTH CRYSTAL DRIVE ARLINGTON, VA 22202

CASE #: OCI-AR-2012-CAC-0037 CROSS REFERENCE #:

TITLE: COMPROMISE OF EPA

SYSTEMS (FO)

**CASE AGENT** (if different from prepared by):

#### SHORT-FORM REPORT OF INVESTIGATION

**PERIOD COVERED:** FROM 1/12/2012 TO 4/16/2013

STATUS OF CASE: CLOSED INVESTIGATION

**JOINT AGENCIES: FBI** 

**DISTRIBUTION:** SAC

AIGI MICHAEL DAGGETT

File

**PREDICATION:** On January 12, 2012, The Office of Cyber Investigations and Homeland Security (OCI) received notification from Page 14, Computer Incident Security Response Center (CSIRC), RTP, NC that an EPA system from Region 4 was suspected to have been compromised by Focused Operations (F0) (5) (7)(E)

**DETAILS:** Due to the sensitive nature of the investigation, the details are not being reported in our electronic case management system. See the hard copy case file for the closing report of investigation.

<u>Allegation 1</u>: Title 18 USC SEC 1029 Fraud and related activity in connection with access devices.

Allegation 1 Findings: See hard copy case file

Allegation 2: Title 18 USC SEC 1030 Fraud and related activity in connection with computers.

Allegation 1 Findings: See hard copy case file

**DISPOSITION:** Investigation was not able to determine the identity of the intruders. A referral for prosecution was not made.



## UNITED STATES ENVIRONMENTAL PROTECTION AGENCY OFFICE OF INSPECTOR GENERAL

TWO POTOMAC YARD 2733 SOUTH CRYSTAL DRIVE ARLINGTON, VA 22202

CASE #: OCI-AR-2012-CAC-0038 CROSS REFERENCE #:

TITLE: COMPROMISE OF EPA

SYSTEMS (FO)

CASE AGENT (if different from prepared by):

#### SHORT-FORM REPORT OF INVESTIGATION

**PERIOD COVERED:** FROM 1/12/2012 TO 4/16/2013

STATUS OF CASE: CLOSED INVESTIGATION

JOINT AGENCIES: FBI

DISTRIBUTION: SAC

AIGI MICHAEL DAGGETT

File

PREDICATION: On January 12, 2012, Chief of Cyber Investigations, Office of Cyber Investigations and Homeland Security (OCI) received notification from Computer Security Incident Response Center (CSIRC) that the US Computer Emergency Response Team (US-CERT) reported an EPA system located in RTP, NC had been compromised by Focused Operations (F0).

**DETAILS:** Due to the sensitive nature of the investigation, the details are not being reported in our electronic case management system. See the hard copy case file for the closing report of investigation.

<u>Allegation 1</u>: Title 18 USC SEC 1029 Fraud and related activity in connection with access devices.

Allegation 1 Findings: See hard copy case file

Allegation 2: Title 18 USC SEC 1030 Fraud and related activity in connection with computers.

Allegation 1 Findings: See hard copy case file

**DISPOSITION:** Investigation was not able to determine the identity of the intruders. A referral for prosecution was not made.





## UNITED STATES ENVIRONMENTAL PROTECTION AGENCY OFFICE OF INSPECTOR GENERAL

DATE: April 11, 2013	PREPARED BY:

CASE #: OCI-AR-2012-CAC-0086 CROSS REFERENCE #:

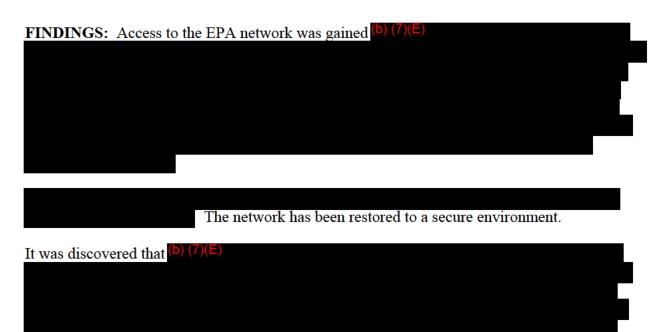
TITLE: COMPRAMISE OF EPA NETWORK SECURITY

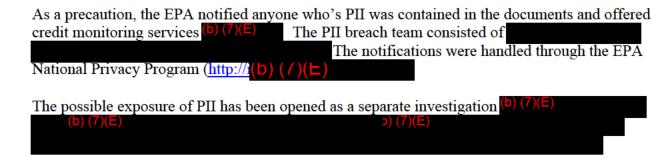
#### CASE CLOSING REPORT

Subject(s)	Location	Other Data
Unknown		

#### VIOLATION(S): Computer Intrusion

ALLEGATION: On April 2, 2012, the Environmental Protection Agency, Office of Inspector General, Office of Cyber Investigations and Homeland Security received notification from EPA Computer Security Incident Response Center, RTP, NC, that numerous EPA systems were being targeted and compromised by unknown individuals and the computers were communicating to known malicious websites.





**DISPOSITION:** As the malware was removed, the network secured, no indication that data was removed and no reports of significant impacts to Agency operations, it is recommended that the investigation into the intrusion be closed. The Electronic Crimes Division will continue (b) (7)(E)



Narrative

#### UNITED STATES ENVIRONMENTAL PROTECTION AGENCY OFFICE OF THE INSPECTOR GENERAL OFFICE OF INVESTIGATIONS

TWO POTOMAC YARD 2733 SOUTH CRYSTAL DRIVE ARLINGTON, VA 22202

#### FINAL REPORT OF INVESTIGATION CONCERNING

#### SECURITY BREACH OF EPA MYPAY SYSTEM OCI-AR-2012-CAC-0146

#### TABLE OF CONTENTS

Section A

Entities and Individuals Prosecution Status Exhibits	Section B Section C	
Distribution: File	Submitted By:	
	Special Agent Electronic Crimes Division Office of Investigations Approved By:	
	Special Agent in Charge Electronic Crimes Division Office of Investigations	

#### OFFICE OF INSPECTOR GENERAL OFFICE OF INVESTIGATIONS

CASE NO.: OCI-AR-2012-CAC-0146 **DATE OPENED:** 

07/23/2012

CASE TITLE: SECURITY BREACH

> OF EPA MYPAY SYSTEM LAST UPDATED:

CASE CATEGORY: COMPUTER INTRUSION CASE AGENT:

JOINT AGENCIES: None **OFFICE:** OCI

JURISDICTION: VIRGINIA

#### SECTION A - NARRATIVE

#### Predication

An investigation was opened on July 23, 2012 based on information received from the Environmental Protection Agency (EPA), Computer Security Incident Response Center (CSIRC), Research Triangle Park, North Carolina. The investigation was initiated as a result of an EPA Employee alleging MyPay account was potentially compromised.

#### Possible violations:

- 1. TITLE 18 USC SEC 1030, Fraud and related activity in connection with computers.
- 2. TITLE 18 USC SEC 1029, Fraud and related activity in connection with access devices.

#### Impact/Dollar Loss

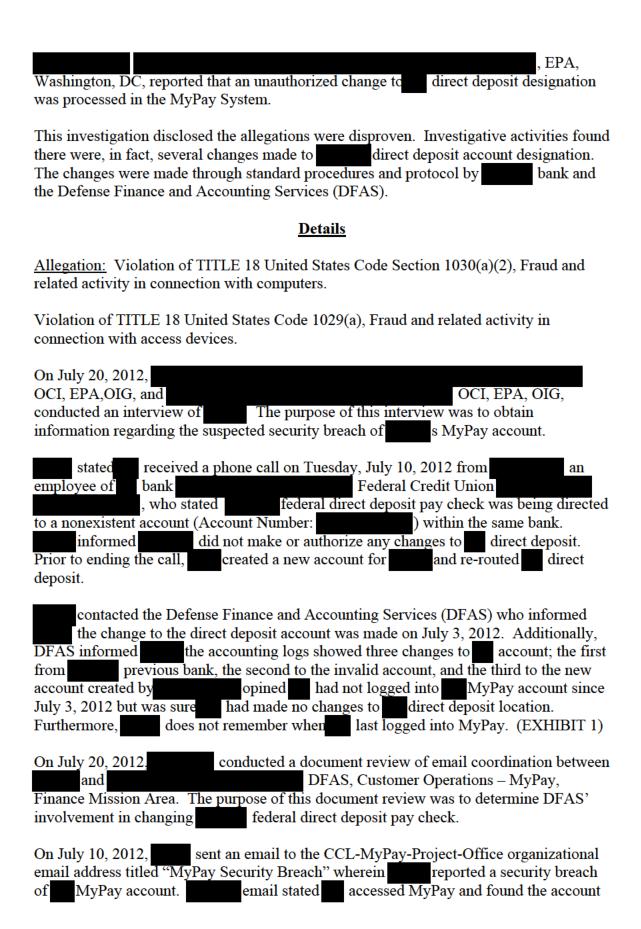
No Dollar loss was sustained by the Government.

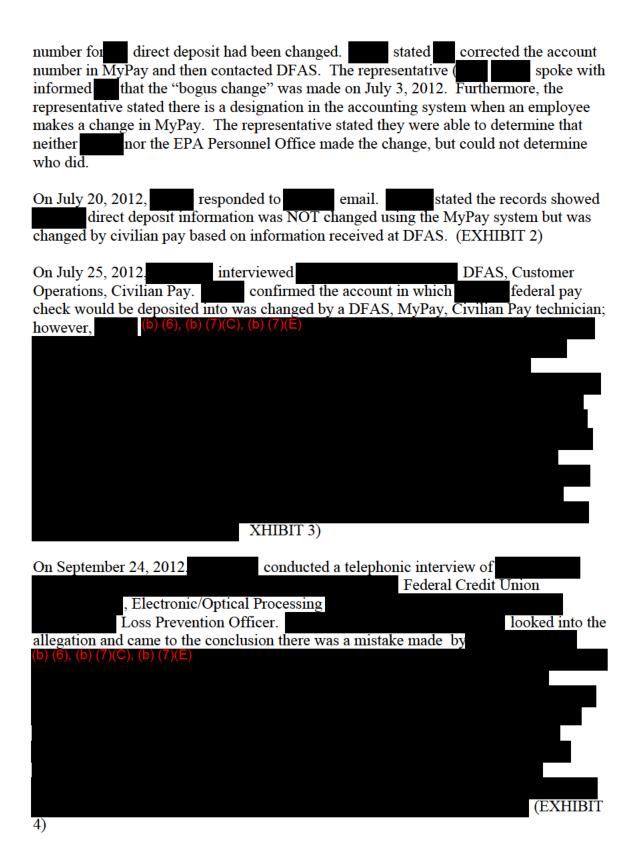
There were no impacts to EPA systems, programs, or processes.

#### Synopsis

On July 12, 2012,	, CSIRC, Office of
<b>Environmental Information</b>	(OEI), EPA, Research Technology Park, North Carolina,
notified	, EPA Office of Inspector General (OIG)
Office of Cyber Investigation	ns (OCI), via email, of a reported security breach to an EPA
employee's pay account on t	the EPA's MyPay System. The EPA employee,

This report is the property of the EPA Office of Inspector General, Office of Investigations and is loaned to your agency. It and its contents may not be reproduced or disclosed without written permission. This report contains information protected by the Privacy Act and is FOR OFFICIAL USE ONLY. Disclosure of this report to unauthorized persons is prohibited. See 5 U.S.C. 552a.





#### **Disposition**

This investigation disclosed all allegations were disproven and no criminal activity occurred. There were no attempts to defraud the government or government employees and there were no connected security breaches to the EPA MyPay System.

#### SECTION B - ENTITIES AND INDIVIDUALS

Name:

Role: Victim

**EPA Employee:** Y

**Business Address:** Ariel Rios South, Room 1200 Pennsylvania Avenue, N.W.,

Washington, DC 20406

**Business Phone: 202** 

#### **SECTION C - PROSECUTION STATUS**

ADMIN/CRIMINAL/CIVIL ACTION(S): As the allegation was disproven and no criminal activity was identified this case was not referred for action.

#### **EXHIBITS**

DESCRIPTION		EXHIBIT
MOI-07/26/2012 -		1
MOA-07/24/2012 –	: Email to DFAS	2
MOI-07/26/2012 —		3
MOI - 10/09/2012 -	and	4



Narrative

**Entities and Individuals** 

# UNITED STATES ENVIRONMENTAL PROTECTION AGENCY OFFICE OF THE INSPECTOR GENERAL OFFICE OF INVESTIGATIONS

TWO POTOMAC YARD 2733 SOUTH CRYSTAL DRIVE ARLINGTON, VA 22202

#### FINAL REPORT OF INVESTIGATION CONCERNING

BREACH OF REGION SERVER OCI-AR-2012-CAC-0147

#### TABLE OF CONTENTS

Section A

Section B

Prosecution Status Exhibits	Section C	
Distribution: File	Submitted By:	
	Special Agent Electronic Crimes Division Office of Investigations Approved By:	
	Special Agent in Charge Electronic Crimes Division Office of Investigations	

## OFFICE OF INSPECTOR GENERAL OFFICE OF INVESTIGATIONS

CASE NO.: OCI-AR-2012-CAC-0147 DATE OPENED:

07/25/2012

CASE TITLE: BREACH OF

REGION SERVER LAST UPDATED:

CASE CATEGORY: COMPUTER INTRUSION CASE AGENT:

JOINT AGENCIES: None OFFICE: ECD

JURISDICTION:

#### **SECTION A - NARRATIVE**

#### **Predication**

An investigation was opened on July 25, 2012, based on information received from the Environmental Protection Agency, Computer Security Incident Response Center, Research Triangle Park, North Carolina. The investigation was initiated as a result of an EPA Information Security Officer reporting a breach of security resulting in unauthorized changes being made to a Region server.

#### Possible violations:

TITLE 18 USC SEC 1030, Fraud and related activity in connection with computers.

#### Impact/Dollar Loss

No Dollar loss was sustained by the Government.

There were no significant impacts to EPA systems, programs, or processes.

#### **Synopsis**

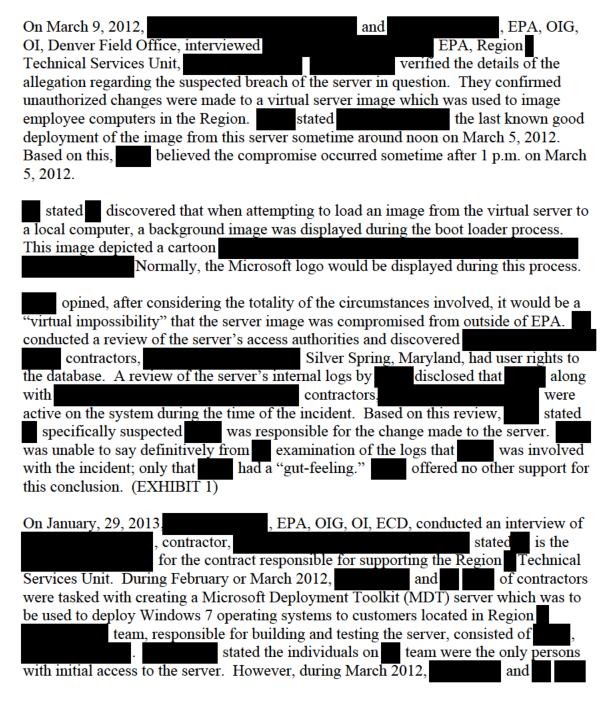
On March 6, 2012, CSIRC, Office of Environmental Information, EPA, Research Triangle Park, North Carolina, notified EPA, Office of Inspector General, Office of Investigations, Electronic Crimes Division, of the possible breach of an EPA Region server by an unidentified person. Specifically, the breach consisted of unauthorized changes being made to the Region server.

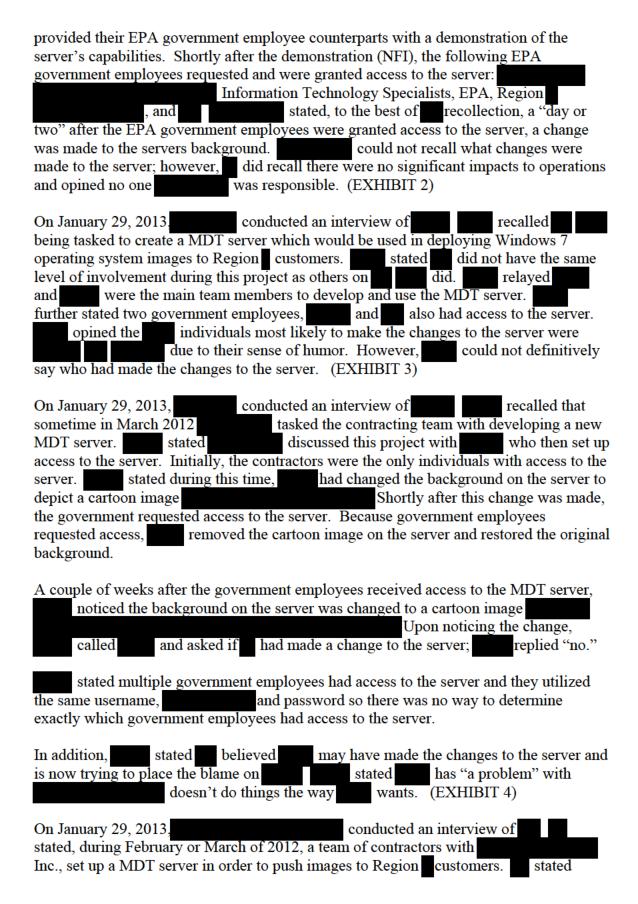
This report is the property of the EPA Office of Inspector General, Office of Investigations and is loaned to your agency. It and its contents may not be reproduced or disclosed without written permission. This report contains information protected by the Privacy Act and is FOR OFFICIAL USE ONLY. Disclosure of this report to unauthorized persons is prohibited. See 5 U.S.C. 552a.

This investigation disclosed the allegations were proven. Investigative activities found there were, in fact, changes made to the server's desktop background. However, the investigation found no criminal activity or malicious intent related to this incident.

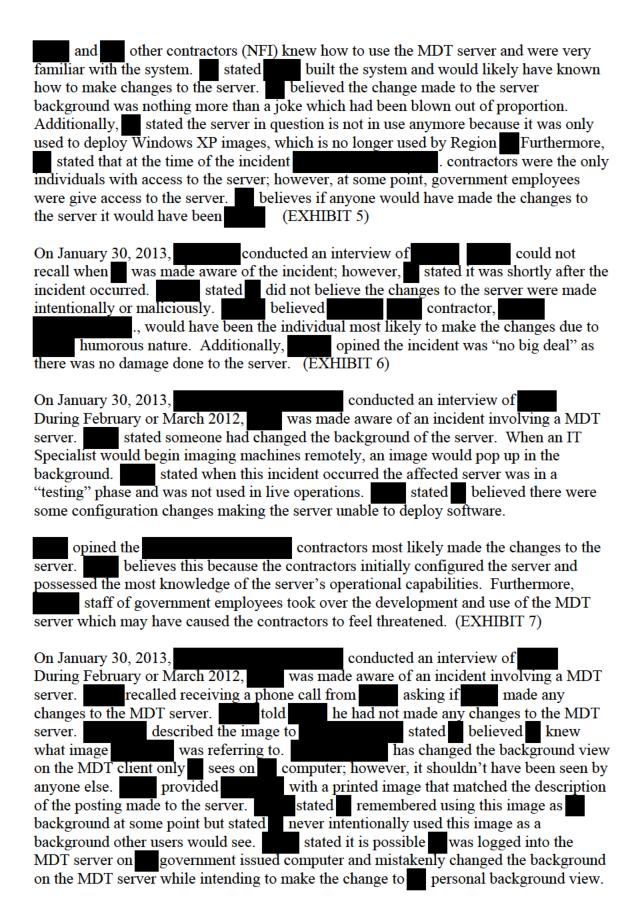
#### **Details**

<u>Allegation:</u> Violation of TITLE 18 United States Code Section 1030(a)(5), Fraud and related activity in connection with computers.





This report is the property of the EPA Office of Inspector General, Office of Investigations and is loaned to your agency. It and its contents may not be reproduced or disclosed without written permission. This report contains information protected by the Privacy Act and is FOR OFFICIAL USE ONLY. Disclosure of this report to unauthorized persons is prohibited. See 5 U.S.C. 552a.



explained that durin	g the course of	work	multiple prod	esses running on
government issued con	nputer. st	ated if was c	onducting wo	ork on the MDT
through the MDT applicat	ion on gover	rnment issued co	omputer	ould have
accidentally changed the b	ackground on th	he MDT applica	tion rather th	an desktop.
maintained this was	not intentional.	(EXHIBIT 8)		

#### **Disposition**

This investigation disclosed the allegation was proven; however, no criminal or malicious activities were found to have occurred to intrude upon, breach security within, or compromise EPA systems.

#### SECTION B - ENTITIES AND INDIVIDUALS

#### **SECTION C - PROSECUTION STATUS**

ADMIN/CRIMINAL/CIVIL ACTION(S): As there was no criminal activity discovered during this investigation this case was not referred for action.

#### **EXHIBITS**

DESCRIPTION	EXHIBIT
MOI-03/09/2012 –	1
MOI-01/29/2013 —	2
MOI-01/29/2013 —	3
MOI-01/29/2013 —	4
MOI-01/29/2013 –	5
MOI-01/30/2013 —	6
MOI-01/30/2013 –	7
MOI-01/30/2013 —	8



<b>DATE:</b> July 24, 2013	PREPARED BY:

CASE #: OCI-AR-2012-CAC-0153 CROSS REFERENCE #:

TITLE: UNNKNOWN SUBJECT: EXPOSURE OF PII DATA IN CONNECTION TO EPA

NETWORK INTRUSION

#### CASE CLOSING REPORT

Subject(s)	Location	Other Data
Unknown		

#### VIOLATION(S): Computer Intrusion

ALLEGATION: On April 2, 2012, The Office of Cyber Investigations and Homeland Security (OCI) received notification from EPA Computer Security Incident Response Center (CSIRC), RTP, NC, that numerous EPA systems were being targeted and compromised by unknown individuals and that the systems were communicating to known malicious websites. Personally Identifiable Information (PII) was resident on one of the compromised servers and it was feared the PII could have been compromised.

<b>FINDINGS:</b>	Access to the EPA network was gained (b) (7)(E)	
It was discov	ered that (b) (7)(E)	

RESTRICTED INFORMATION

This report is the property of the Office of Investigations and is loaned to your agency: it and its contents may not be reproduced without written permission. The report is FOR OFFICIAL USE ONLY and its disclosure to unauthorized persons is prohibited. Public availability to be determined under 5 U.S.C. 552.

### 



1301 CONSTITUTION AVE., NW WASHINGTON, DC 20004

<b>DATE:</b> MAY 31, 2013	PREPARED BY:	
CASE #: OCI-HQ-2011-CAC-12	ASE #: OCI-HQ-2011-CAC-1229 CROSS REFERENCE #:	
TITLE: UNAUTHORIZED AC	CESS TO GOVERNMENT SYS	STEMS
COMP	LAINT SUMMARY REP	ORT
Subject(s)	Location	Other Data
Unknown		
Security received notification that Computer Emergency Response 7 pertaining to an EPA contractor.  On December 6, 2010,	Feam that contained EPA domain interviewed	
home computer being compromis contained EPA data and reported	to the Agency.	investigation related to ed by the US CERT that
that all accounts, except webm be compromised by malware. steps to try and detect the malwar with Malware Bytes and a few of	e on system.	ceiving information they may ne details and conducted some related scanned system
INVESTIGATIVE FINDINGS: revealed (b) (7)(E), (b) (7)(C), (b) (6) other pieces well as numerous other suspicious	of malware were identified and r	resident on computer as
Investigation revealed that multiple pieces of malicious softw		ter that was infected with rendered inoperative.

#### RECOMMENDATION: (b) (5)

this investigation should be closed. The threat to the EPA has been mitigated and further analysis of malware discovered would be an inefficient use of limited resources.



## UNITED STATES ENVIRONMENTAL PROTECTION AGENCY OFFICE OF THE INSPECTOR GENERAL OFFICE OF INVESTIGATIONS

TWO POTOMAC YARD 2733 SOUTH CRYSTAL DRIVE ARLINGTON, VA 22202

Special Agent in Charge

#### FINAL REPORT OF INVESTIGATION CONCERNING

	ONINTO MULTIPLE WORKSTATIONS (b) (7)(E)  OCI-RTP-2012-CAC-0062  TABLE OF CONTENTS
Narrative Entities and Individuals Prosecutive Status Exhibits	Section A Section B Section C
Distribution: SAC File	Approvals:

### OFFICE OF INSPECTOR GENERAL OFFICE OF INVESTIGATIONS

**CASE AGENT:** 

CASE NO.: OCI-AR-2012-CAC-0062 DATE OPENED: 02/24/2012

CASE TITLE: UNKNOWN SUBJECT: INTRUSIONINTO

INTRUSIONINTO MULTIPLE WORKSTATIONS (5) (7)(E)



CASE CATEGORY: COMPUTER INTRUSION OFFICE:

OFFICE OF CYBER INVESTIGATIONS AND HOMELAND SECURITY - IMMEDIATE OFFICE

JOINT AGENCIES: Federal Bureau of

Investigation

JURISDICTION: N/A

#### **SECTION A - NARRATIVE**

#### **Predication**

On February 16, 2012, Spe	ecial Agent	, United States Enviro	nment Protection
Agency, Office of Inspecto	r General, Office of Investig	ations, Region 4, Resea	rch Triangle Park field
office, received a complaint	from		Office of Technology
Operations and Planning, an	nd Technology Information S	Security Staff,	, pertaining
to an intrusion of the Office	of the Administrator,	computer, an	d the Office of Air and
Radiation,	computer.		

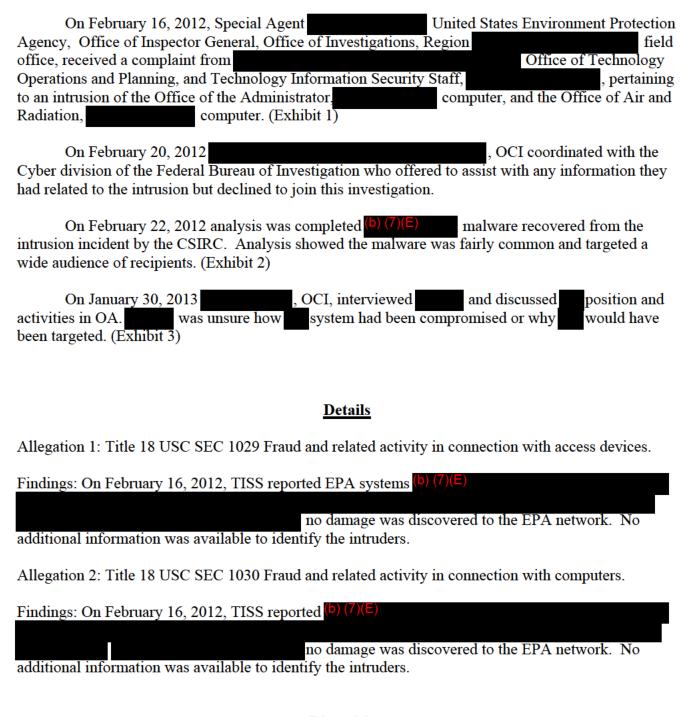
#### Possible violations:

- 1. TITLE 18 USC SEC 1029, Fraud and related activity in connection with access devices
- 2. TITLE 18 USC SEC 1030, Fraud and related activity in connection with computers

#### **Impact/Dollar Loss**

This incident impacted the security and stability of the EPA local area network and EPA Senior Level administration operations.

#### **Synopsis**



#### **Disposition**

Investigation was not able to determine the identity of the intruders. A referral for prosecution was not made.

#### SECTION B - ENTITIES AND INDIVIDUALS

Name of Person: Unknown

Title & Company: Role: Subject Business Address: Business Phone: EPA Employee: N

-----

#### **SECTION C – PROSECUTIVE STATUS**

ADMIN/CRIMINAL/CIVIL ACTION(S): None

#### **EXHIBITS**

DESCRIPTION	EXHIBIT
Case Initiation	1
MOA Malware Analysis	2
MOI Interview of	3



<b>DATE:</b> September 13, 2013	PREPARED BY:			
CASE #: OI-HQ-2013-CAC-0	091 CROSS REFEREN	CROSS REFERENCE #:		
TITLE: COMPROMISE OF V	WWW. (b) (7)(E)	EBSITE SERVERS		
	CASE CLOSING REPORT	Γ		
Subject(s)	Location	Other Data		
UNKNOWN				
VIOLATION(S): 18 USC § 10 COMPUTERS	030 - FRAUD AND RELATED A	CTIVITY IN CONNECTION WITH		
Investigations, Electronic Crime	mental Protection Agency, Office es Division, received information comised on April 30, 2013. The w	that the www ov		
The website had to be taken off	line for several days while triaged	d and analyzed. <mark>(b) (7)(E)</mark>		
FINDINGS: ECD made arrang analysis. It was determined that www gov. (b) (7)(E)	gements to image the servers and to the servers and to the servers and to the servers and the servers are servers as the servers and the servers are servers as the servers and the servers and the servers are servers as the servers and the servers and the servers are servers as the servers and the servers are servers as the servers and the servers are servers as the se	to provide copies to CSIRC for		
(b) (7)(E)				
(b) (7)(E)				
	LPS, Inc. 1744 West Katella Ave file/). VLPS is a hosting and sup			

virtual and cloud computing. VLPS has facilities in California and Virginia. The American

Registry for Internet Numbers (ARIN) indicates that this IP address is allocated to the Asian Pacific Network Information Centre (APNIC) and is registered in Thailand.

is registered to Ubiquity Server Solutions, 12101 Tukwila International Blvd., Tukwila, WA 98168 (https://www.ubiquityservers.com/seattle-data-center). Ubiquity is a server hosting company providing dedicated and cloud computing, the Seattle data center provides service for the Western United States, Canada, and Asia.

is registered to Pacific Internet, Taikoo Shing, Island East, Hong Kong (www.Pacnet.com). Pacnet owns and operates complete network systems throughout Asia, including data hosting and servicing.

Forensic analysis also identified one destination where it looked lik (b) (7)(E)

(b) (7)(E) is owned by AT&T Internet Services, 2701 N. Central Expressway, Richardson, TX, 75080, and is a "Direct Allocation." According to AT&T the designation as "Direct Allocation" indicates the server is wholly controlled by a separate entity. An IG subpoena was issued to AT&T Internet Services to determine ownership of the destination server.

An email response was delivered on June 28, 2013 in response to an Inspector General subpoena issued to AT&T Internet Services, Legal Compliance Group, 1010 N. St. Mary's Street, Room 315-A2, San Antonio, TX 78215, Fax (707) 435-6409, served on June 18, 2013. The response indicated that AT&T had no records pertaining to IP address (b) (7)(E)

Further research identified the IP address belongs to a sub-division of AT&T. According to the Domain Dossier service, the Registrant is SBC Internet Service, Inc., 12976 Hollenberg Drive, Bridgeton, MO 63044 and the administrative contact is

AT&T Internet Services Compliance Officer, confirmed that information regarding the IP address was not available because AT&T Internet Services has no record of this IP address having been assigned/provisioned to any subscriber. The only record(s) regarding this IP address are that it appears to have been staged for future provisioning for AT&T U-verse subscribers.

Inquiries with other cyber law enforcement and intelligence agencies did not provide any viable leads or indication that information was exfiltrated from the (b) (7)(E)

**DISPOSITION:** It is recommended this case be closed due to lack of investigative leads, no confirmation that data was exfiltrated and the probability that further investigation will be not produce results.



DATE: February 8, 2013 PREPARED BY: SA

CASE #: OI-AR-2012-CAC-0206 CROSS REFERENCE #:

TITLE: UNAUTHORIZED USE OF EPA CREDENTIALS / MISREPRESENTATION OF

**GOVERNMENT OFFICIAL** 

#### **CASE CLOSING REPORT**

Subject(s)	Location	Other Data
UNSUB	UNKNOWN	
VIOLATION(S):		
` ,		
NONE		
ALLEGATION:		
NONE		
FINDINGS:		
NONE		
DISPOSITION:		

Administratively closed. Two case numbers inadvertently assigned to one incident in IGEMS. For additional information pertaining to this investigation, please refer to EPA OIG Case #: OI-AR-2012-CAC-0207

UNAUTHORIZED USE OF EPA CREDENTIALS / MISREPRESENTATION OF GOVERNMENT OFFICIAL



# UNITED STATES ENVIRONMENTAL PROTECTION AGENCY OFFICE OF INSPECTOR GENERAL OFFICE OF INVESTIGATIONS

1595 WYNKOOP STREET, 4<sup>th</sup> FLOOR DENVER, CO 80202

**DATE:** March 19, 2013 **PREPARED BY:** 

CASE #: 2009-CS-0085 CROSS REFERENCE #:

**TITLE: LIBBY SUPERFUND SITE** 

#### CASE CLOSING REPORT

Subject(s)	Location	Other Data
Unknown	Libby, Montana	
	EPA Region 8, Denver,	
	Colorado	
	EPA Headquarters,	
	Washington, D.C.	

#### **VIOLATION(S):**

18 U.S.C. § 242 (Deprivation of Right Under Color of Law)

18 U.S.C. § 371 (Conspiracy to Commit Offense or to Defraud the United States)

18 U.S.C. § 1001 (False Statements)

18 U.S.C. § 1341 (Mail Fraud)

18 U.S.C. § 1343 (Wire Fraud)

18 U.S.C. § 1346 (Scheme or Artifice to Defraud [Honest Services])

**ALLEGATION:** An allegation was received that unknown EPA officials violated the civil rights of the citizens of Libby, Montana, by not performing required scientific testing to determine the safe expose level to Libby amphibole asbestos; released written information to the public stating their homes were safe when they (unknown EPA officials) knew the homes could still be contaminated and present a danger to the citizens of Libby; and EPA officials failed to provide honest services to the citizens of Libby, Montana, in the clean-up of asbestos from the W.R. Grace mine that may have contaminated the town of Libby, Montana.

**FINDINGS:** Interviews of EPA personnel (to include EPA scientists) and hundreds of residents of Libby, Montana; and a review of documentation associated with the allegations in question were conducted. The investigation demonstrated that the EPA proceeded in the clean-up of attic insulation under an Emergency Response Removal Action (ERRA) in violation of the requirements of the Comprehensive Environmental Response, Compensation and Liability Act (CERCLA) and proceeded to perform remediation activities without conducting the required Baseline Risk Assessment.

**DISPOSITION:** This investigation was referred to the United States Attorney's Office (USAO) in Great Falls, Montana, for possible criminal prosecution. The USAO declined prosecution based on (b) (5)

All actions and remedies have been addressed, and no further investigative activity is warranted. This case is closed.